Steps toward improved analysis for Network Mission Assurance

Craig M. Burris, Jimmie G. McEver, Heather W. Schoenborn, and David T. Signori

Abstract— **The DoD focus on Joint network-enabled operations promises benefits in terms of improved force agility and effectiveness; however, the greater dependence on network capability makes it imperative that DoD decision makers understand the impact of such capabilities on mission success. This paper proposes a new analytic approach aimed initially at achieving first-order network mission assurance assessments by modeling aggregate behavior at a low level of resolution. It is based on the premise that risk of mission failure due to degradation of C2 is driven by the degree of dependency on key underlying functions (i.e., information sharing, collaboration, and direction) enabled by the common networks and the ability of these network to support such functions in realistic threat environments. It employs risk functions of different shapes and scales that relate the capability of links among groups of users to risk of failure of mission tasks. This paper describes the applicable problem space, the methodology, and outstanding research challenges.**

Index Terms—**cyber measurement, net enabled C2, network analysis, network performance, mission assurance.**

I. Introduction

TODAY the US is faced with a very complex and uncertain national security environment, with threats that vary from terrorism and insurgency to major nation states [1]. The DoD strategy for dealing with this environment is to transform to a net enabled agile force that can span the full spectrum of crisis and conflict, ranging from natural disasters through irregular warfare to major conventional operations. However, it is recognized at the highest levels in DoD that to be successful in this endeavor, commanders must be provided with a Joint Network they can rely upon to gain a decisive advantage over adversaries – one that is resilient to attack and robust in performance across the full range of situations that might be encountered. Commanders need to be assured that they can achieve success in missions that depend on the network.

This so-called Network Mission Assurance[1] poses great challenges for decision makers at all levels and, in particular, for the analysts that advise them. They grapple with questions such as how much capability is enough to ensure mission success, and how might degraded network performance impact the force's ability to employ preferred methods, accomplish essential tasks, and achieve desired end states and mission objectives; or ultimately how to balance costs with level of risk to mission failure? Because of the critical role of the Joint Network in the national security strategy [2], it is important to understand the impact of network capability on mission success when making key decisions related to investment, system engineering and operation or even force employment.

Commercial industry quantifies the competitive advantage afforded by their enabling networks. There are a host of network-based innovations intended to attract and keep customers [3]. When evolving such enterprises companies attempt to understand not only the role of their networks in gaining competitive advantage but also how the size and performance of their network contributes to their bottom line, their measure of mission success [4]. DoD, which admittedly differs from commercial industry in some important ways, has struggled for years to relate information systems, in contrast to weapons systems, to mission outcome. Decision-makers have often been forced to resort to *ad hoc* prioritization of requirements that bubble up from below with little quantitative understanding of how the related programs contribute to mission success. The result was that often network capability was considered expendable overhead easily traded off for more weapon systems. However, the central role of an integrated and global Joint Network in enabling force agility and providing a platform for cyber operations has positioned it as a weapon system that demands its contribution to the mission be better understood and quantified to improve decision making and mission outcomes.

Manuscript received May 21, 2010. This work was supported in part by the Office of the Assistant Secretary of Defense for Networks and Information Integration under Contract N00024-03-D-6606, Task CTP02.

C. M. Burris is with the Johns Hopkins University Applied Physics Laboratory, Applied Information Sciences, 21-S200, 11100 Johns Hopkins Rd., Laurel, MD 20723 USA (phone: 703-699-3458; fax 703-699-3012; email: craig.burris@jhuapl.edu).

J. G. McEver is with Evidence Based Research, Inc., 1595 Spring Hill Road, Suite 250, Vienna, VA 22182 USA (email: mcever@ebrinc.com).

D. T. Signori is with Evidence Based Research, Inc., 1595 Spring Hill Road, Suite 250, Vienna, VA 22182 USA (email: signori@ebrinc.com).

H. W. Schoenborn is with the Office of the Assistant Secretary of Defense for Networks and Information Integration, 1550 Crystal Drive, Suite 1000, Arlington, VA 22202 USA (email: heather.schoenborn@osd.mil).

[1] The approach and tools described in this paper began with and evolved from work done in support of the Mission Assurance Program Decision Memorandum (PDM) Study completed in 2009 under the leadership of PA&E (now CAPE) and OASD/NII. The term Network Mission Assurance (NMA) highlights the focus on estimating risk arising from the failure to provide adequate network capability, or the degradation of network capability due to attack or failure – rather than from all sources of operational risk.

978-0-7695-4211-9/10 $26.00 © 2010 IEEE
DOI 10.1109/SocialCom.2010.175

Report Documentation Page	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE **MAY 2010**	2. REPORT TYPE	3. DATES COVERED **00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE **Steps toward improved analysis for Network Mission Assurance**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Office of the Assistant Secretary of Defense for Networks and Information Integr,1550 Crystal Drive, Suite 1000,Arlington,VA,22202**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S) 11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

2nd IEEE International Conference on Social Computing / IEEE International Conference on Privacy, Security, Risk and Trust, Bloomington, MN, 20-22 Aug 2010

14. ABSTRACT

The DoD focus on Joint network-enabled operations promises benefits in terms of improved force agility and effectiveness; however, the greater dependence on network capability makes it imperative that DoD decision makers understand the impact of such capabilities on mission success. This paper proposes a new analytic approach aimed initially at achieving first-order network mission assurance assessments by modeling aggregate behavior at a low level of resolution. It is based on the premise that risk of mission failure due to degradation of C2 is driven by the degree of dependency on key underlying functions (i.e., information sharing, collaboration and direction) enabled by the common networks and the ability of these network to support such functions in realistic threat environments. It employs risk functions of different shapes and scales that relate the capability of links among groups of users to risk of failure of mission tasks. This paper describes the applicable problem space, the methodology, and outstanding research challenges.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**6**	

II. The Nature of the Problem

Unfortunately, the heavier reliance on a common-user network[2] characterized by shared resources and the need to address capabilities from an enterprise wide perspective pose even greater challenges for analysts. The first big challenge is "The Curse of Dimensionality". When viewed on a DoD wide basis, there is a broad range of situations, operations, missions, tasks and functions to consider. Forces associated with the various Services often have different information support needs, as do the Command and Control (C2), Intelligence and Logistics communities that support them. There is a spectrum of operational threats that can be expected against the network. The Joint Network is comprised of several functional domains and a large number of information system programs. Finally, both the users and providers reflect a multiplicity of cultures, terminology and perspectives, all of which must be considered when seeking viable solutions.

The second major problem is the difficulty of forecasting demand for network capability. It is characterized by deep uncertainty. Due to the dynamic and uncertain nature of operational environments shaped by human behavior, information exchange requirements are continually changing. Adversaries adopt new Tactics, Techniques and Procedures (TTPs), the equivalent of business processes in commercial industry, to counter successful strategies. Warfighters must respond to the resulting surprises by adapting their own TTPs. Technology and business processes co-evolve in unpredictable ways; users discover innovative ways of using new information system capabilities and these new methods give rise to requirements for additional information system capabilities. In the large analysts are faced with a broad, multidimensional, heterogeneous, complex system-of systems operating in a highly uncertain environment.

Although there exists an array of techniques and tools that can be used to address selected aspects of this problem, a comprehensive methodology that addresses the full scope of the problem set has proven elusive. The most commonly used methods rely on stating requirements for exchange of information among users or their supporting information systems; i.e. Information Exchange Requirements, or so called IERs. However, related methods and tools have significant limitations that can degrade the quality of decisions regarding capabilities that affect large numbers of network users or the DoD enterprise as a whole. When estimating the demand for aggregate network capabilities, metrics for various domains are often inconsistent and values for the same domains can vary widely due to heavy reliance on inputs from Subject matter Experts (SMEs) who are limited by their specific operational experiences. Steps necessary to aggregate IERs quickly explode as the number of users increase. When estimating network capabilities that can be supplied, analysts are often forced to resort to databases containing the acquisition requirements for specific programs versus network capabilities. Also, methods to aggregate programs into network capability tend to be immature; particularly when the effects of loading, network vulnerabilities and an array of threats must be considered.

Methods for relating aggregate network capability to operational outcome emphasize the use of detailed operational threads based on IERs for specific operational situations. This approach can be very fragile when dealing with dynamically changing environments and poses major dimensionality challenges when attempting to deal with the range of possibilities. Combat models intended to address mission effectiveness generally represent network capabilities very weakly and in different ways. When coupled with more detailed network models, they require extensive time and resources to apply. Because of these limitations, the result is often decisions being made without an adequate understanding of the potential impact on the network as a whole or the implications for the missions it will support.

III. Creating a New Analytical Support Environment

To be able to address the overarching analytical challenge there is a need for a common framework with consistent metrics, a quantifiable, repeatable methodology and a supporting family of tools that allow tailoring to a wide range of needs in a timely and responsive manner. The necessary change in capability is summarized in Fig. 1. In order to overcome the formidable impediments described earlier and achieve this vision, a fundamentally new approach is required.

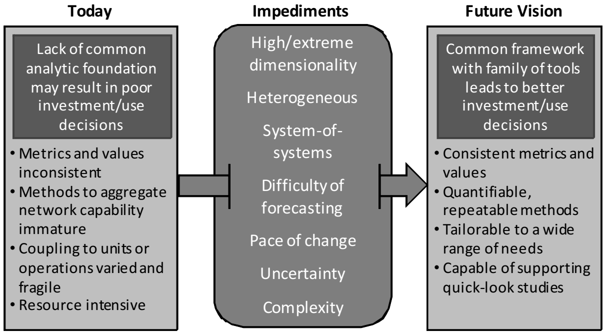
Today
Lack of common analytic foundation may result in poor investment/use decisions
• Metrics and values inconsistent
• Methods to aggregate network capability immature
• Coupling to units or operations varied and fragile
• Resource intensive
Impediments
High/extreme dimensionality
Heterogeneous
System-of-systems
Difficulty of forecasting
Pace of change
Uncertainty
Complexity
Future Vision
Common framework with family of tools leads to better investment/use decisions
• Consistent metrics and values
• Quantifiable, repeatable methods
• Tailorable to a wide range of needs
• Capable of supporting quick-look studies

Figure 1. The Analytic Challenge: Rapidly determining how much network capability is enough to assure mission success.

To overcome the dimensionality challenge inherent in an enterprise-wide framework and exacerbated by the historical IER-based approach, we propose to aim, initially, for an 80-90% solution by modeling aggregate capability at a low but consistent level of resolution that is useful to support some of the important investment and resource allocation decisions of interest in DoD today. That is, the approach uses a relatively small set of key dimensions and driving variables to model network capability demand, supply and the mission implications of gaps in capability.

This approach trades precision for tractability. It permits the

[2] Also referred to as "the Joint Network" to reflect DoD's intent to move away from Service-specific network implementations and toward integrated (or at least interoperable), enterprise-wide networking capabilities.

rapid generation of aggregate estimates and the identification of major shortfalls. As necessary more detailed analyses can then be focused in the most important areas. The key is a model-building approach that attempts to choose dimensions and variables that are the major drivers; that is explicitly examine and discard factors whose impact on aggregated capability is small (e.g. less than one percent).

IV. The End-to-End Process

Fig. 2 illustrates the major steps of the top level NMA analytical process and the key question addressed by each step. These include estimating aggregate demand to determine how much capability is needed; estimating available, programmed or planned capability that can be supplied to assess its adequacy; and determining the mission risk in terms of the likelihood of mission failure given the associated shortfalls identified in the previous step.

To obtain methods and tools that enable this process requires fundamental change in the basic premises that underlay each step of the approach. These hypotheses and their implications are summarized below:

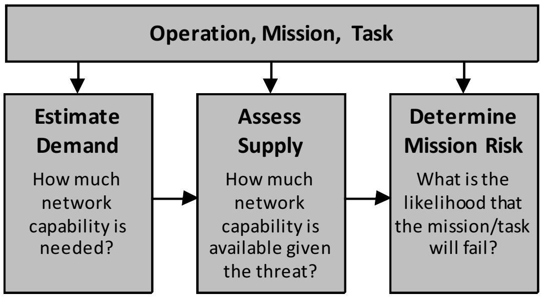
Operation, Mission, Task
Estimate Demand
How much network capability is needed?
Assess Supply
How much network capability is available given the threat?
Determine Mission Risk
What is the likelihood that the mission/task will fail?

Figure 2. Key steps in top level NMA analytical process.

1) *The aggregate demand for network capability is driven by trends in communication devices.* This permits the user demand to be modeled using the expected device characteristics and a few key parameters. When combined with unit information and a tractable aggregation scheme it provides the basis for an operationally tailorable, enterprise-wide database that can be used to estimate network capability demand for various force structures. Note that the level of demand required may vary with mission type, and the demand database must provide the level of demand associated with the minimum needed to accomplish all the critical tasks associated with the mission in question. Thus, demand is calculated at a level where there is no excess that may be re-allocated between tasks, because doing so for a particular task would increase risk for another.
2) *Capability supplied by a network can be estimated with sufficient accuracy by aggregating the capability of the programs or systems that support a unit for a particular mission.* A practical aggregation scheme that can be applied to multiple devices and programs in a manner consistent with the demand framework permits direct supply and demand comparisons.
3) *Mission effectiveness and risk of mission failure are driven by the degree to which essential tasks are dependent on key functions enabled by the Joint Network; e.g. information sharing, collaboration and direction.* Through the application of network theory this permits rapid building and application of models that relate network capability to risk of task failure.

The overall approach to modeling is to establish a methodological framework that permits flexible linking and tailoring of the models for each step to the operational context and data available for the problem being addressed. The modeling approach for each step is described below.

1) Model network demand as the aggregate demand of classes of users in units who support the mission by employing various types of devices connected to the Joint Network. Select only the device types and level of demand needed for the particular mission tasks to be assessed. For example, in some tasks only wireless man-portable devices may be relevant;
2) Model the supply of network capability as the aggregate of program supply for those Joint Network related programs supporting users in a unit. For instance, model the effective bandwidth provided for a particular device type when operating in a subnet structure appropriate for the mission, and aggregate the capacity of this device with similar devices at the unit level. Apply appropriate environmental and threat conditions to degrade the available supply from ideal levels;
3) Model mission impact by relating effective performance of links among groups of users to risk of failure of mission critical tasks. Account for the network structure of users and links in each critical task, as well as the fact that most critical tasks are not entirely dependent on the Joint Network. Repeat the process for each critical task necessary for mission success.

V. Assessing Network-Based Risk

Having described the end-to-end method for estimating network demand, assessing network capability, and determining the resulting mission-task risk, it is worthwhile to describe the risk assessment framework and method in more detail. The basic approach relies on a risk estimation framework to establish a mathematical relationship between mission critical tasks and network degradation as measured by the fraction of relevant unit-to-unit logical links that do not have adequate capacity, and thus pose risk to these tasks. This relationship is in terms of a curve (referred to as a risk curve) that captures the increase in the chance of task failure with the loss of supporting links.

A. Basis for the Risk Curves

The underlying premise of this method is that the risk of mission failure is driven by the degree to which essential mission tasks are dependent on the performance of the organizational (logical) networks that enable specific C2-related functions: information sharing, collaboration and direction [5, 6]. Each one of these three logical networks has a distinct form appropriate for the function enabled by the network as depicted in Fig. 3. These functions can be viewed as progressively enabling segments of the well-known Observe-Orient-Decide-Act (OODA) loop, although other C2 process representations may be used as well [7]. That is: *information sharing* is critical to the ability to observe and orient (situation awareness); *collaboration* with multiple actors is often necessary to continually orient and decide (or plan adaptively), particularly in complex endeavors; and when necessary, specific *direction* is required to maintain positive command and control in support of task execution [8]. All elements of the OODA loop are needed for most tasks/missions; however, all do not have to be network-enabled for task success [9]. For each task to be assessed, it is important to establish which segments of the OODA loop (and therefore which of information sharing, collaboration, and direction functions) have critical network dependency for task success [10].

B. *Building Risk Curves*

The roles that logical networks play in each of the three key functions described above emphasize different structural properties and topologies, even though all three may be supported by the same underlying infrastructure. Research indicates that these topologies degrade differently as links are degraded, whether from failure, attack or other reasons [10-13]. The result is that risk associated with network failure increases along a relatively predictable path (risk curve) tied to the underlying network structure. The risk curves estimate how well each structure would be able to maintain properties critical to task success as network links are lost. Principles that informed the determination of the impact of network degradation on users conducting a task were as follows:

- Information sharing: Deficient links reduce paths available for information transfer. Since alternate paths are likely to exist, minimum impact would be expected at low levels of degradation but more degradation results in disconnected islands of nodes.
- Collaboration: Deficient links reduce the ability to participate in activities necessary to gain shared understanding. Initial losses have a proportional effect due to the inability to participate in collaborative planning sessions; additional degradation creates widespread increases in network distances between concurrent sessions.
- Direction: Even small numbers of deficient links disrupt the group's ability to act in a dynamic and timely manner, and backup paths provided by redundancy are much less effective.

As indicated in Fig. 3, a family of network topologies and characteristics consistent with the above assumptions were postulated to form the basis for determining the general relationships between the likelihood of mission failure and the fraction of links that are not adequately provisioned. These curves have two major features that must be specified from mission information:

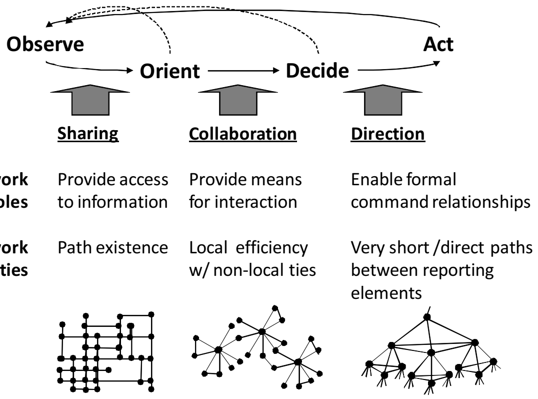
Observe
Act
Orient
Decide
Sharing
Collaboration
Direction
Network Roles
Provide access to information
Provide means for interaction
Enable formal command relationships
Network Properties
Path existence
Local efficiency w/ non-local ties
Very short /direct paths between reporting elements

Figure 3. Network forms mapped to C2 "basis functions" and a representation of a C2 process.

- The *shape* of the curve, which varies with the type of basic function enabling C2 for the task; and
- The *scale* of the curve, which is determined by the degree of dependency of the task on the network-enabled functional capability.

The details of the particular methods used to arrive at the shapes of the curves that relate network degradation to mission risk for each C2 basis function are beyond the scope of this paper, and will be described in other venues [14]. Briefly, they are derived both from relevant network science literature and from simulation explorations of the degradation of key network metrics in network topologies associated with the C2 basis functions discussed above.

Metrics used for the sharing topology included the size of the largest connected component of the network and the size of the largest n-clique in the network, where an n-clique is defined as a maximal cluster of nodes, each of which is connected to every other node in the cluster via a path length of n steps or fewer. N was examined for various values, but practical limits on relaying critical information between nodes will likely limit the value for N to approximately 3 - 4. For collaborative structures and activities, both clustering and short path lengths are important characteristics [15]. These metrics were examined collectively via a metric that divided the clustering coefficient of the network by the mean path length as links were removed from this structure. For directed structures, maintaining direct connection between adjacent nodes is paramount. Alternative routes between nodes can be used, but at significant cost. This relationship was modeled as an order of magnitude degradation in effectiveness as path lengths increase (practically, paths of 3 or greater add no value in enabling command relationships).

Fig. 4 shows some early results of simulations runs for theses metrics as applied to the network structures discussed earlier, as implemented in the NetLogo modeling environment [16]. As network value is lost, risk to the mission/task increases, and thus the shape of operational risk curves can be obtained by inverting network value curves of the type shown in Fig. 4.

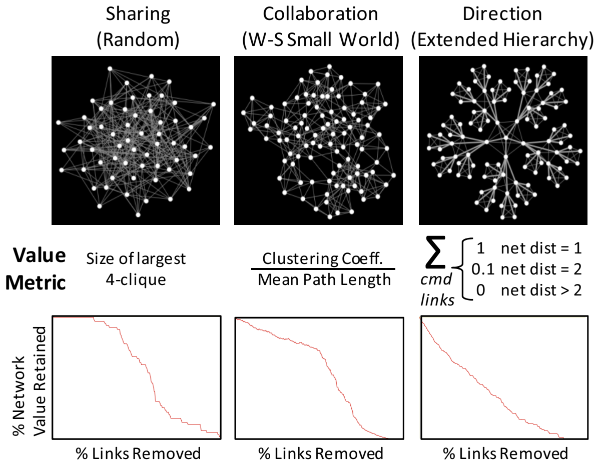

Figure 4. Sample Results of Initial Simulation Efforts

Risk curve scale was determined by estimating the residual ability to accomplish the mission-task without the Joint Network. A method was established based on information typically found in TTPs to estimate the reliance of a critical task on the Joint Network at one of several predetermined levels. If more precise detail is available that would allow selection of a specific limit of risk associated with network reliance, that specific scale may be selected and modeled.

Fig. 5 depicts the process by which mission and task information can be used to select the appropriate curve for use in risk assessment. For the initial study effort, operational concept documents that described plans and relevant TTPs (tactics, techniques and procedures) were used to determine the type and degree of functional dependency. This was accomplished through a mapping of critical operational tasks to functional tasks and sub-tasks that would be performed by the units involved in the mission. TTPs and related doctrine typically specify network dependencies at the functional sub-task level (e.g., Navy use of network resources for Maritime Dynamic Targeting).

C. Use of results: Understanding Implications and Mitigations

In addition to aggregate results at the task-risk level, the methodology was implemented in a way that provided indications of specific logical links that were under-provisioned given particular threat scenarios, providing a means for "diagnosis" of sources of risk. This, in turn, can be mapped to the particular network supply components that provided the infrastructure for these demand links, supporting considerations of various alternatives. In addition, the tools developed for this methodology allowed for parallel comparison of various means to provision adequate link capacity against a range of threats. Results could be formulated on a threat-case by threat-case basis, or could be combined with threat occurrence and success likelihood estimates to produce more aggregate risk assessments. Non-material mitigations could also be considered, particularly at the level of reducing or changing the type of network dependency required for a particular task. Importantly, alternative threats and mitigations could be considered in terms of operational risk, a scale that is both common to different types of capability, and quantified in a currency that is aligned with the value generated by these technologies and the organizations and processes in which they are embedded.

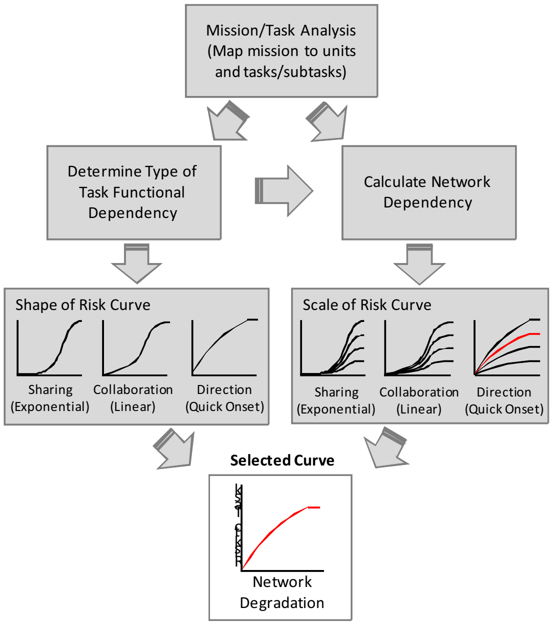

Figure 5. Overview of the NMA Risk Mapping Methodology

VI. Emerging Methods/Tools/Data and Continuing Research Challenges

The initial version of the methods, tools and data outlined above have been prototyped and applied, under some practical ground rules: minimize complexity and apply to real problems early; and evolve the capability based on resulting lessons and the demands of the type of issues that remain to be addressed. The current status of these efforts is summarized below:

1) Estimating demand: A set of device metrics and values for various classes of users have been compiled. Aggregation rules have been developed to permit the estimation of demand for related land, sea and air users within DoD. These elements have been incorporated into a web based tool that permits flexible parsing and stochastic sensitivity analysis. The results have been compared with those from several independent requirements studies and successfully rationalized.
2) Assessing supply: a multilevel methodology that accounts for the interaction among programs to different degrees has been developed. The methodology has been applied to several problems of interest to DoD. As application expands, inputs from supporting tools may be appropriate. Some tools have been reviewed and identified for this purpose.

3) Determining mission risk: a family of models characterizing task impact due to the loss of links that support C2-related functions has been developed, along with the criteria for selecting a model appropriate for a specific task context. Work is underway to expand upon initial results to improve understanding of applicable metrics for various network structures.

While these initial efforts suggest that the methods, tools, and data could have wide applicability across DoD, much remains to be done to establish the vision outlined here. A number of refinements in the demand model are under development including the extension of the user/unit structure to facilitate demand estimates for Irregular Warfare. Improved methods for parsing demand, relating it to programs and addressing fully the impact of demand-based loading on supply estimates are candidates for development. The theoretical basis for and implementation of the risk-curve models is being refined. However, the credibility and hence utility of these methods and tools depend upon the degree of review and acceptance by peers. To this end a series papers dealing with the details of each of the key steps in the top level NMA analysis process (estimating demand [17], assessing supply [18] and determining risk [14, 19]) are being published to increase awareness, point out areas of research needed to mature these capabilities and solicit feedback that would help improve their soundness and utility.

Acknowledgments

The authors wish to acknowledge the significant contributions of individuals and groups who supported this work. The authors are grateful to the following individuals for their contributions to the technical content of this work; from the Johns Hopkins University Applied Physics Laboratory: Paul Kim, Mary Ann Hendrickson, Michael Morris, Steve Sudkamp and Keith Wichmann; from Evidence Based Research, Inc.: Christine Anderson, Ayanah George, Heather Noell and Karl Selke; from RAND: Dan Gonzales, Isaac Porche and Bradley Wilson; from Telcordia: Darrell Woelk; and from the Northwestern University Center for Connected Learning and Computer-Based Modeling: Forrest Stonedahl.

References

[1] Office of the Secretary of Defense, *Quadriennial Defense Review*, 2010.

[2] Office of the Secretary of Defense, *DoD Information Management & Information Technology Strategic Plan* 2008-2009.

[3] Friedman, Thomas L., *The World is Flat; A Brief History of the 21st Century*, Picardi Reading Group Guide, 2007.

[4] Straussman, Paul A., *The Business Value of Computers, Information Economics Press*, New Canaan, Connecticut, 1990, pp. 225-251.

[5] D. Alberts and R. Hayes, *Understanding Command and Control*, The Future of Command Series, U.S. DoD Command and Control Research Program, 2006

[6] J. Gartska and D. Alberts, *Network Centric Operations Conceptual Framework 2.0*, U.S. Office of Force Transformation and Office of the Secretary of Defense for Networks and Information Integration, 2004.

[7] *Marine Corps Doctrinal Publication 1, Warfighting*, Department of the Navy, June 1997.

[8] R. Hayes, "It's an Endeavor, Not a Force," The International C2 Journal, 2007, http://www.dodccrp.org/html4/journal_v1n1.html, accessed 22 April 2010.

[9] NATO SAS-065 Research Task Group, NATO *Network Enabled Command and Control Maturity Model*, Final Report, Prepared for NATO, 2009.

[10] R. Albert and A. Barabasi, "The Statistical Mechanics of Complex Networks," *Reviews of Modern Physics*, Vol. 74, January 2002.

[11] K. Carley, J. Less, and D. Krackhardt, "Destabilizing Networks," *Connections* **24(**3), 2001.

[12] R. Albert, H. Jeong, and A. Barabasi, "Error and Attack Tolerance of Complex Networks," *Nature* **406,** 378-382, 2000.

[13] P. Crucitti, V. Latora, M. Marchiori and A. Rapisarda, "Error and Attack Tolerance of Complex Networks," *Physica A* **340**, 388-394, 2004.

[14] C. Burris, J. McEver, H. Schoenborn and D. Signori, "Estimating Operational Risk Associated with Network Performance," *Proceedings of the 78th MORS Symposium*, June 2010, submitted for publication.

[15] V. Latora and M. Marchiori, "Efficient behavior of small-world networks," *Phys. Rev. Lett.* **87**, 198701 (2001).

[16] Wilensky, U. (1999). NetLogo. http://ccl.northwestern.edu/netlogo/. Center for Connected Learning and Computer-Based Modeling, Northwestern University, Evanston, IL.

[17] C. Burris et al, "Quantitative Capability Delivery Increments (QCDI) demand model: a novel approach for estimating future DoD network needs," *Proceedings of the 15th International Command and Control Research and Technology Symposium*, U.S. DoD Command and Control Research Program, Santa Monica, CA, June 2010, in press.

[18] C. Burris, D. Gonzales, J. McEver, D. Signori, M. Smeltzer and H. Schoenborn, Quantitative Capability Delivery Increments: a novel approach for assessing DoD network capability, *Proceedings of the AIAA InfoTech@Aerospace Conference*, American Institute of Aeronautics and Astronautics, April 2010.

[19] C. Burris, J. McEver, H. Schoenborn and D. Signori, "Network Mission Assurance: A novel approach for estimating the degree of mission risk from network vulnerabilities," *Proceedings of MILCOM 2010*, submitted for publication.

Craig M. Burris is a Technical Lead and Project Manager for network analysis in the Applied Information Sciences Department at the Johns Hopkins University Applied Physics Laboratory. Prior to his current assignment, he spent more than 20 years designing, installing, and managing operational networks. He earned a B.S. in Electrical Engineering from the U.S. Naval Academy in 1987, and a Masters in Military Studies from the Marine Corps University in 2000.

Jimmie G. McEver is a Scientist and Program Manager in the C3 Futures Program at Evidence Based Research, Inc. His current research focuses on command and control, network-enabled operations, complex adaptive systems and network science. He earned a Ph.D. in Physics from the Georgia Institute of Technology, Atlanta, GA in 1997, and a Master of Public Policy from Harvard University, Cambridge, MA, in 1991.

David T. Signori, Jr. is Chief Scientist of the C3 Futures Program at Evidence Based Research, Inc. His current research focuses on quantitative methods and tools for assessing net-centric capabilities and architecture that enable command and control of forces operating in complex, uncertain and stressed environments. He earned a Ph.D. Electrical Engineering from Michigan State University in 1968, and served in senior executive positions with the Defense Information Systems Agency and the Defense Advanced Research Projects Agency.

Heather W. Schoenborn is a Senior Engineer with the Office of the Assistant Secretary of Defense for Networks and Information Integration. For more than 25 years she has performed research and managed programs in remote sensing, knowledge management, and supporting information technology for the Defense Department. She earned Bachelor of Science degrees in Geology and Marine Sciences from the Pennsylvania State University in 1980 and a Master of Science in Civil Engineering from the Virginia Polytechnic Institute and State University in 1991.